

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re U.S. Patent Application)
)
Applicant: Takayoshi Kurita)
)
Serial No.)
)
Filed: March 14, 2001)
)
For: SMART CARD ACCESS)
MANAGEMENT SYSTEM,)
SHARING METHOD, AND)
STORAGE MEDIUM)
)
Art Unit:)

I hereby certify that this paper is being deposited with the United States Postal Service as EXPRESS MAIL in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231, on March 14, 2001.

Express Label No.: EL 846162085 US

Signature:

T. Kurita

CLAIM FOR PRIORITY

Assistant Commissioner for Patents
Washington, DC 20231

Sir:

Applicant claims foreign priority benefits under 35 U.S.C. § 119 on the basis of the foreign application identified below:

Japanese Patent Application No. 2000-269096, filed September 5, 2000.

A certified copy of the priority document is enclosed.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By

Patrick G. Burns
Reg. No. 29,367

March 14, 2001
300 South Wacker Drive
Suite 2500
Chicago, IL 60606
(312) 360-0080
Customer Number: 24978

#2



PATANT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the
following application as filed with this Office.

Date of Application: September 5, 2000

Application Number: Patent Application
No. 2000-269096

Applicant(s): FUJITSU LIMITED

December 1, 2000

Commissioner,
Patent Office Kozo OIKAWA

Certificate No. 2000-3098184

1503.65307
(312) 360-0080

#2

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

J1017 U.S. PTO
09/809736
03/14/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 9月 5日

出 願 番 号

Application Number:

特願2000-269096

出 願 人

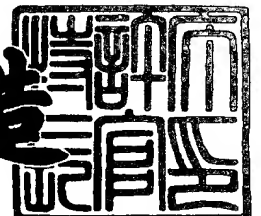
Applicant(s):

富士通株式会社

2000年12月 1日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2000-3098184

【書類名】 特許願

【整理番号】 0051322

【提出日】 平成12年 9月 5日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/00

【発明の名称】 スマートカードのアクセス管理システム、共有方法及び記憶媒体

【請求項の数】 10

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 栗田 享佳

【特許出願人】

 【識別番号】 000005223

 【氏名又は名称】 富士通株式会社

【代理人】

 【識別番号】 100074099

 【住所又は居所】 東京都千代田区二番町8番地20 二番町ビル3F

 【弁理士】

 【氏名又は名称】 大菅 義之

 【電話番号】 03-3238-0031

【選任した代理人】

 【識別番号】 100067987

 【住所又は居所】 神奈川県横浜市鶴見区北寺尾7-25-28-503

 【弁理士】

 【氏名又は名称】 久木元 彰

 【電話番号】 045-573-3683

【手数料の表示】

 【予納台帳番号】 012542

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705047

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 スマートカードのアクセス管理システム、共有方法及び記憶媒体

【特許請求の範囲】

【請求項 1】 複数のアプリケーションによるスマートカードへのアクセスを管理するスマートカードのアクセス管理システムであって、

アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャンネルが存在すれば、該アプリケーションを排他獲得済みとする排他制御手段と

排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可するアクセス制御手段と

を備えることを特徴とするアクセス管理システム。

【請求項 2】 前記排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャンネルが存在しなければ、該排他獲得要求を行ったアプリケーションをキューに登録することを特徴とする請求項 1 に記載のアクセス管理システム。

【請求項 3】 前記アクセス制御手段は、前記アクセス要求に対し、前記排他を獲得したアプリケーションが前記スマートカードから未認証である時、該アプリケーションの要求を拒否することを特徴とする請求項 1 又は 2 に記載のアクセス管理システム。

【請求項 4】 前記アクセス制御手段は、前記スマートカードがスマートカードリーダーより抜かれた時、該抜かれたスマートカードにより認証済みとなっているアプリケーションを未認証に変更することを特徴とする請求項 1 乃至 3 のいずれか 1 に記載のアクセス管理システム。

【請求項 5】 前記アプリケーションは、前記スマートカードに複数回アクセ

スする時、各アクセスの開始時に前記排他制御手段に前記排他獲得要求を行い、該各アクセスの終了時に前記排他制御手段に排他の解除通知を行うことを特徴とする請求項 1 乃至 4 のいずれか 1 に記載のアクセス管理システム。

【請求項 6】 前記排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードが他のアプリケーションによって既に排他獲得済みであれば、該排他獲得要求を行ったアプリケーションをキューに登録し、前記アプリケーションからの排他の解除通知に対し、前記キューに登録されているアプリケーションを排他獲得済みとすることを特徴とする請求項 5 に記載のアクセス管理システム。

【請求項 7】 前記アクセス制御手段は、アプリケーションからスマートカードの認証解除の通知に対し、該認証解除が該スマートカードにより認証済みとなっている最後のアプリケーションからの時、該スマートカードに認証解除を要求することを特徴とする請求項 1 乃至 6 のいずれか 1 に記載のアクセス管理システム。

【請求項 8】 複数のアプリケーションによるスマートカードへのアクセスを管理するスマートカードの共有方法であって、

アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャンネルが存在すれば、該アプリケーションを排他獲得済みとし、

排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可することを特徴とする共有方法。

【請求項 9】 1 つのスマートカードへの複数のアクセス処理を含むアプリケーション又はそのライブラリであって、

前記各アクセス処理に対し、該アクセス処理の開始時にそれぞれ前記排他獲得要求を行い、各アクセス処理の終了時にそれぞれ排他の解除通知し、

前記複数のアクセス処理のうちの最初の処理時のみに該アクセス処理を行うスマートカードに対して認証要求を行うことを特徴とするアプリケーション又はそ

のライブラリ。

【請求項 1 0】 複数のアプリケーションが並列動作する情報処理装置によって使用された時、

アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとし、

排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可することを前記情報処理装置に行わせるプログラムを記憶した前記情報処理装置が読み出し可能な記録媒体。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、スマートカード上のデータの複数プロセスによる共有した場合のスマートカードのアクセス管理に関する。

【 0 0 0 2 】

【従来の技術】

スマートカードは、従来用いられている磁気カードに比して非常に大きな容量のデータを記憶することが出来ることなどから、様々な分野への使用が検討され、あるいは実用化されている。

【 0 0 0 3 】

またスマートカードは、内部にメモリ共に CPU を備えており、この CPU を介してメモリ内のデータへアクセスを行うので、アクセス時に CPU に認証処理を行わせることにより、従来の磁気カードに比べて高いセキュリティ性を実現出来、この点もスマートカードのメリットとなっている。

【 0 0 0 4 】

スマートカードは PIN (Personal Identification Number) によるセキュリティ機能を持っており、この機能により PIN の照合を行い、認証された場合に

だけカード内の秘密情報をアクセスすることができるように制御することが可能である。この P I N による認証は、いわゆるパスワード入力方式で、スマートカードを用いるユーザが P I N として例えばパスワードを入力し、これをスマートカード内に記憶しているパスワードとカード内で比較して、一致した場合に内部データへのアクセスを許可する。

【 0 0 0 5 】

スマートカードへのアクセスは、スマートカードが持つ論理チャネルを通して行い、認証要求は論理チャネルに対して行われる。そしてスマートカードは、この論理チャネル毎に P I N による認証状態などセキュリティに関する状態を保持している。

【 0 0 0 6 】

図 1 5 は、アプリケーションから見たスマートカード内部の論理的構成を示したものである。

スマートカード内では、データをツリー構造の構成によって管理しており、最上位にある D I R の下層に、使用されるアプリケーション毎の単位等で D F (Delicated File) が設けられている。そして、各 D F 内には実際のデータを保持している E F (Elementary File) が格納されている。スマートカードからデータを読み出す際、アプリケーションは、まずアクセスを行うデータの位置を示す位置付け情報を送って、目的の E F にアクセス位置を移動した後、その E F からデータの読みだし／書込みを行う。また各チャネルは、現在のアクセス位置を状態情報として保持している。

【 0 0 0 7 】

【発明が解決しようとする課題】

現在スマートカードを複数のアプリケーションで同時に使用する使い方が検討されている。例えば公開鍵暗号方式をベースとした P K I (Public Key Infrastructure) システムを構築し、このシステム上のコンピュータで複数のアプリケーションが稼動している場合に、各アプリケーションがデジタル署名などによるセキュリティ認証にスマートカードを用いることが、現在スマートカードの 1 つの使用方法として考えられている。

【 0 0 0 8 】

この場合、スマートカードを接続したコンピュータ上の複数のアプリケーションがスマートカードを共用することになる。そして多数のアプリケーションに同一のカードに対してアクセスさせる場合、1つのスマートカードが持つ論理チャネルの数はせいぜい2チャネル程度なので、1つの論理チャネルを複数のアプリケーションが共有する必要があるが出てくる。尚本明細書内の以下の説明は、説明の簡略化のため、1つのアプリケーションは1つのプロセスで構成されることを前提としており、アプリケーションという言葉のプロセスと同義で用いている。通常1つのアプリケーションは1つのプロセスで構成されることが多いが、複数のプロセスで構成されている場合でも、アプリケーションをプロセスと置換えて考えれば、以下の説明は基本的に同じである。

【 0 0 0 9 】

現行のスマートカードのセキュリティ方式では、1つのアプリケーションがある論理チャネルに対してP I N 認証を行いアクセス許可を得ると、以降その論理チャネルからは、認証が解除されるまでの間、認証を受けたアプリケーションだけでなく他のアプリケーションもアクセス出来てしまう。

【 0 0 1 0 】

複数のアプリケーションで1つのカードの同じ情報を共有することを、セキュリティの観点から考えると、個々のアプリケーション毎にP I N による認証を行った方がセキュリティレベルはより強固になる。しかし、現行のスマートカードへのアクセス制御では、1つの論理チャネルを複数のアプリケーションで共有する場合、論理チャネル毎に認証が行われ各論理チャネルに認証状態（アクセス許可を与えたか否か）が保持されるため、1つのアプリケーションがP I N による認証を行ってアクセス許可を得れば、他のアプリケーションはP I N による認証を受けずに、その論理チャネルからカードへのアクセスが可能となってしまう。

【 0 0 1 1 】

また、各上述したように各アプリケーションは、カード内のデータにアクセスする際、位置付け情報を論理チャネルに送信してアクセス位置を移動してからデータの書込み／読みだしを行うが、複数のアプリケーションが論理チャネルを共

有する場合、各アプリケーションはカレントのアクセス位置の把握が難しくなる。

【 0 0 1 2 】

上記問題点を鑑み、本発明は、複数のアプリケーション（プロセス）によるアクセスに対し、スマートカードへの認証状態を一元管理することにより、各アプリケーション（プロセス）毎に認証許可を与えるスマートカードのアクセス管理システム及び管理方法を提供することを課題とする。また、各アプリケーション（プロセス）毎の認証を認証処理によるオーバーヘッドを大きくすること無く実現するアクセス管理システム及び管理方法を提供することを課題とする。

【 0 0 1 3 】

【課題を解決するための手段】

上記問題点を解決するため、本発明によるスマートカードのアクセス管理システムは、複数のアプリケーションによるスマートカードへのアクセスを管理するものであって、排他制御手段及びアクセス制御手段を備える。

【 0 0 1 4 】

排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとする。また上記排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在しなければ、該排他獲得要求を行ったアプリケーションをキューに登録する。

【 0 0 1 5 】

アクセス制御手段は、排他獲得済みとなっているアプリケーションからの上記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可する。またアクセス制御手段は、上記アクセス要求に対し、上記排他を獲得したアプリケーションが上記スマートカードから未認証である時、該アプリケーションに P I N の入

力を要求する。各アプリケーションによるスマートカードの認証はこのアクセス制御手段を通して行われ、アクセス制御手段は各アプリケーションとスマートカードとの認証関係を把握している。

【0016】

本発明によれば、排他制御手段により、スマートカードに対する排他制御が行われるので、複数のアプリケーションによってスマートカードを共用しても各アプリケーション毎の認証を可能とする。

【0017】

また、アクセス制御手段により、各アクセス要求を行ったアプリケーションが認証済みかどうか判断され、認証済みの場合、認証処理を行わずにアクセス許可を与えるので、認証処理回数を削減することが出来る。

【0018】

【発明の実施の形態】

以下に本発明の一実施形態について、図面を参照しながら説明する。

各アプリケーション毎に認証許可を与えるようにするためには、スマートカード（スマートカードが複数の論理チャネルをもつ場合論理チャネル）に対して排他制御を行い、認証された1つのアプリケーションがスマートカードを使用している間、そのアプリケーションがカード（若しくは論理チャネル）を専有し、他のアプリケーションからのアクセスを抑止する必要がある。尚説明簡略化の為、以下の実施形態では各スマートカードは論理チャネルを1つ備える構成とする。尚スマートカードが複数論理チャネルを備えた場合は、以下に説明する排他制御は論理チャネル単位で行われる。

【0019】

図1は、排他制御機構を設け、スマートカードにアクセスするアプリケーションの排他処理を行った場合を示す。

図1では、複数のアプリケーション21とスマートカード22の間に排他制御機構11を設け、スマートカード22に対してアクセスを要求する際、各アプリケーション21はこの排他制御機構11に対して排他獲得要求を行い、排他が得られたアプリケーション21が、スマートカード22を専有してアクセスを行う

。同図の排他制御機構 1 1 はカード a、b の 2 つのカードへのアクセスに対する排他を管理している。そしてアプリ 1、アプリ 2 及びアプリ 3 の 3 つのアプリケーション 2 1 がカード a に対してアクセス要求を発行しており、排他制御機構 1 1 はそのうちのアプリ 1 に対して排他獲得とし、他のアプリ 2 及び 3 はカード a が解放されるまで待ち状態にしておく。排他を獲得したアプリ 1 は、カード a の論理チャネルに対して P I N 認証を行った後データの読みだし／書込みを行う。この間他のアプリケーション 2 1 は、カード a に対してアクセスすることが出来ない。アプリ 1 が処理を完了してカード a を解放すると、次に、待ち状態となっているアプリ 2 が排他を獲得し、カード a に対して P I N 認証を行った後内部のデータにアクセスする。この様に排他制御機構 1 1 を設けることにより、認証を受けた 1 つのアプリケーションのみスマートカードに対してアクセスすることが出来、各アプリケーション 2 1 毎の認証を実現することが出来る。

【 0 0 2 0 】

この図 1 の構成による方式の場合、1 つのアプリケーション 2 1 がスマートカード 2 2 を使用している間このスマートカード 2 2 はこのアプリケーション 2 1 に専有されるので、他のアプリケーション 2 1 は排他が解除されスマートカード 2 2 が解放されるまで待ち状態になる。よってこの方式では、複数のアプリケーションの並列処理性能が悪く、また待ち状態にあるアプリケーションは長い期間処理を停止してハングアップした状態に見える等、非常に使い勝手が悪くなる。

【 0 0 2 1 】

これを回避するものとしては、アプリケーション 2 1 がスマートカード 2 2 へのアクセス処理が完了すると専有していたスマートカード 2 2 を逐一解放する方式がある。この方式では、アプリケーション 2 1 が複数回スマートカード 2 2 に対するアクセス処理を含む場合、各アクセス処理毎に排他制御機構 1 1 に対してスマートカード 2 2 への排他獲得／解放を行い、こまめに排他制御を区切る。

【 0 0 2 2 】

図 2 に、この方式による各アプリケーションのスマートカードへの排他獲得／解放の例を示す。

同図は、図 1 と同様アプリ 1、アプリ 2 及びアプリ 3 の 3 つのアプリケーション

ン 2 1 がカード a に対してアクセス要求を発行した場合の各アプリケーションのスマートカードへのアクセス処理例を示すもので、同図中排他制御機構 1 1 への矢印↑は、各アプリケーション 2 1 から排他制御機構 1 1 への排他獲得要求、排他制御機構 1 1 からの矢印↓は排他制御機構 1 1 から各アプリケーション 2 1 への排他獲得の通知を示す。また斜線部分は各アプリケーション 2 1 による P I N 認証処理、網掛け部分はスマートカード 2 2 へアクセス処理を示す。

【 0 0 2 3 】

排他を獲得したアプリケーション 2 1 が、全処理が完了するまで排他を解除してスマートカード 2 2 を解放しなかった場合、アプリ 2 は排他制御機構 1 1 にカード a への排他獲得要求を行った図 2 中の 3 1 の位置から、既にカード a への排他を獲得しているアプリ 1 が処理が完了する 3 3 の位置まで、更にアプリ 3 は 3 2 の位置からこのアプリ 2 の処理が完了するまで待ち状態となる。しかし、同図の様にアプリケーション 2 1 が各アクセス処理毎にこまめに排他制御を区切ることで、排他が解除された期間に別のアプリケーション 2 1 がカード a にアクセスすることが出来るので、排他獲得の為の待ち状態となり処理が停止してしまう期間が短くなり、処理の並列性が向上する。

【 0 0 2 4 】

この様に、排他制御を頻繁に切替えると、各アプリケーションの待ち状態の期間は短くなり処理の並列性は向上する。しかし図 2 の斜線部に示すように各アプリケーションは切替えの度に認証状態の設定／解除処理を行う必要があり、その為のオーバーヘッドが大きくなってしまう。また認証の再許可を得る際 P I N を送信するので、各アプリケーション 2 1 が P I N を保持し続けることになり、セキュリティ上の問題も生じる。これを回避するため、認証処理の度にユーザがパスワードを入力する構成とすると更に認証処理のオーバーヘッドが大きくなる。

【 0 0 2 5 】

図 3 にこの点を考慮した構成を示す。

図 3 の構成では、複数のアプリケーション 2 1 とスマートカード 2 2 の間に、排他制御機構 1 1 に加えアクセス制御機構 1 2 を設け、このアクセス制御機構 1 2 によって各アプリケーション 2 1 のスマートカード 2 2 による認証を一元管理

しながら、排他制御機構 1 1 がスマートカード 2 2 にアクセスするアプリケーション 2 1 の排他処理を行っている。

【 0 0 2 6 】

各アプリケーション 2 1 はスマートカード 2 2 に対してアクセスを要求する際、まず排他制御機構 1 1 に対して排他獲得要求を行い、排他が獲得できると次にアクセス制御機構 1 2 にスマートカード 2 2 への認証を依頼する。そして認証が得られるとスマートカード 2 2 内のデータにアクセスする。

【 0 0 2 7 】

アクセス制御機構 1 2 は認証状態管理テーブルを持ち、この認証状態管理テーブルを用いてアプリケーション 2 1 がスマートカード 2 2 への認証の開始宣言を行ってから認証の解除を通知するまでの間について各アプリケーションとスマートカード 2 2 との認証状態の管理を行う。

【 0 0 2 8 】

図 4 は、認証状態管理テーブルの構成例を示す図である。

認証状態管理テーブルは、各アプリケーション 2 1 が現在どのスマートカード 2 2 から認証を得ているのかを排他制御機構 1 1 が管理するために用いるテーブルで、アプリ識別情報と認証済みカード情報を対応づけて記憶している。アプリ識別情報は、各アプリケーション 2 1 を識別するための一意な識別子を記憶するもので、この識別子は、一般のアプリケーションが操作できないものが用いられ、例えばプロセス生成時に各プロセスに付加され、カーネルが管理しているプロセス ID を用いる。あるいは、スマートカードへアクセスへのアクセス要求を行ったアプリケーション 2 1 に対してアクセス制御機構 1 2 が識別子を順次生成付加してゆく構成としてもよい。

【 0 0 2 9 】

図 4 はカード a, b の 2 つのスマートカード 2 2 に対する各アプリケーション 2 1 の認証状態を管理する場合を例示しており、各アプリケーションに対し認証済みカード情報としてそのアプリケーション 2 1 が認証されているカードが記録されている。尚認証済みカード情報が空欄の部分は、そのアプリケーションに対し認証済みとなっているスマートカードが存在しないことを示す。同図では、ア

プリ 1 はカード a, b 両方が認証済み、アプリ 2、アプリ n はいずれも未認証、アプリ 3 はカード a のみ認証済みとなっている。

【 0 0 3 0 】

各アプリケーション 2 1 は、スマートカード 2 2 に対する認証及びスマートカード 2 2 へのアクセスをアクセス制御機構 1 2 を介して行う。アプリケーション 2 1 からスマートカード 2 2 へのアクセス要求があると、認証状態管理テーブルを参照してそのアプリケーション 2 1 がアクセス要求したスマートカード 2 2 に認証済みであるかどうかを調べ、未認証ならばアプリケーション 2 1 からの要求を拒絶し、またアプリケーション 2 1 に P I N の入力を要求してスマートカード 2 2 との認証処理を行う。また、そのアプリケーション 2 1 が認証済みならばアプリケーション 2 1 は既にそのスマートカード 2 1 の認証許可を得ているのでスマートカード 2 1 へのアクセスを許可し、実行する。

【 0 0 3 1 】

図 5 はアプリケーション 2 1 がスマートカード 2 2 へのアクセスを行う際の、アプリケーション 2 1、排他制御機構 1 1 及びアクセス制御機構 1 2 の処理の流れを示した図である。同図はアプリ 1 がカード a に対してアクセスを行う場合を例としており、また以下の説明中の 1) ~ 2 3) は図 5 中の番号と対応している。

- 1) アプリ 1 はカード a への排他開始を行うため、排他制御機構 1 1 に対し、排他獲得要求を行う。
- 2) アプリ 1 からの要求に対し、排他制御機構 1 1 は、カード a に対し排他獲得済のアプリケーションが有るか調べ、既に他のアプリケーションが獲得していたならば排他待ちのキューに登録する。また排他獲得済でなければ、アプリ 1 に排他獲得を通知する。
- 3) アプリ 1 は、アクセス制御機構 1 2 にカード a へのアクセス開始宣言を行う。
- 4) アクセス開始宣言に対しアクセス制御機構 1 2 は、認証状態管理テーブルにアプリ 1 を登録する。そして、アプリ 1 に P I N の入力要求を行う。尚アプリ 1 がカード b にもアクセス開始宣言を行っている場合は、アプリ 1 は既に認証状態

管理テーブルに登録してあるのでカード a に対するアクセス開始宣言で再度認証状態管理テーブルに登録する必要はない。

5) アプリ 1 はユーザにパスワードの入力を促し、ユーザの入力から P I N を指定してカード a への認証を要求する。

6) 排他制御機構 1 1 は、カード a に対し P I N を通知し、カード a に認証チェックを行わせる。

7) アクセス制御機構 1 2 は、カード a による認証チェックの結果、認証が得られれば、認証状態管理テーブルにアプリ 1 がカード a に認証済みであることを登録する。

8) アプリ 1 はアクセス制御機構 1 2 に対し、カード a へのデータの読み出し／書込みを要求する。

9) アプリ 1 からの読み出し／書込み要求に対し、認証状態管理テーブルを検索し、アプリ 1 が認証済カード a に認証済みならばカード a に対してアクセスを行う。未認証ならば、アプリ 1 にエラーを通知する。

1 0) 1 つのアクセス処理が完了しカード a の専有を解除する場合に、アプリ 1 は排他制御機構 1 1 に排他の解除を通知する。

1 1) 排他制御機構 1 1 は、登録されているアプリ 1 のカード a に対する排他獲得を削除し、他にカード a への排他待ちのキューに登録されているアプリケーション 2 1 があればそのアプリケーション 2 1 の排他獲得を登録する。

1 2) 排他の解除後、アプリ 1 はカード a へのアクセス処理以外の処理を行う。この間、カード a の排他を解放しているので他のアプリケーション 2 1 がカード a を使用することが出来る。

1 3) アプリ 1 は、再度カード a へのアクセスの必要が生じると、排他制御機構 1 1 に排他獲得要求を行う。

1 4) アプリ 1 からの要求に対し、排他制御機構 1 1 は 2) と同様、カード a に対し排他獲得済のアプリケーションが有るか再度調べ、既に他のアプリケーションが排他獲得済でなければ、アプリ 1 に排他獲得を通知する。

1 5) アプリ 1 はアクセス制御機構 1 2 に対し、カード a へのデータの読み出し／書込みを要求する。

1 6) アクセス制御機構 1 2 は、再度 9) と同様な処理を行う。この時 7) で、認証状態管理テーブルにアプリ 1 がカード a に認証済みであることが登録されているので、そのままカード a へアクセスを行う。以降アプリ 1 内のカード a へのアクセス処理の回数分 1 0) ~ 1 6) の処理が繰り返される。

1 7) 全アクセス処理が完了するとアプリ 1 は、アクセス制御機構 1 2 にカード a への認証を解除を通知する。

1 8) アクセス制御機構 1 2 は、認証状態管理テーブルのアプリ 1 からカード a 認証済の情報を削除する。

1 9) アクセス制御機構 1 2 は、認証状態管理テーブル 1 3 に他にカード a に認証されているアプリケーション 2 1 が存在しなくなるまで認証状態を保持し、認証されているアプリケーション 2 1 存在しなくなるとカード a に認証解除を要求する。これにより同一のスマートカードとの認証処理の回数を削減することが出来る。

2 0) アプリ 1 は、アクセス制御機構 1 2 にスマートカード 2 2 へのアクセス終了を通知する。

2 1) 2 0) での通知を受けるとアクセス制御機構 1 2 は認証状態管理テーブルから、アプリ 1 を削除する。この時アプリ 1 が他のスマートカード 2 2 に対してはまだアクセスを終了していない場合は認証状態管理テーブルからアプリ 1 を削除しない。

2 2) アプリ 1 は排他制御機構 1 1 にカード a の排他の解除を通知する。

2 3) 排他制御機構 1 1 は、再度 1 1) と同様な処理を行い、排他を解除する。

【 0 0 3 2 】

図 6 は、図 3 の排他制御機構 1 1 及びアクセス制御機構 1 2 を備えた構成による各アプリケーションへのスマートカードへの処理を示す図である。

同図は、比較のため図 2 と同じ前提の元での同じアプリケーション 2 1 の処理を示してある。図 6 を図 2 比較すると、各アプリケーション 2 1 は、認証処理としては、一番最初のカード a へのアクセス処理開始時の P I N による認証処理と、一番最後のアクセス処理終了時にカード a への認証の解除処理を行っているのみで、図 2 では行っていたカード a への各アクセス処理毎の認証処理が省略され

ている。よって各アプリケーション 21 は認証処理が省略された分処理時間が短くなる。また各アプリケーション 21 が、カード a を専有している期間も認証処理が省かれた分だけ短くなるので、その分待ち状態となる期間が短くてすむ可能性がある。更に各アプリケーション 21 は、スマートカード 22 に対する P I N 認証を最初に 1 度だけ行えばよいので、カードから認証が得られれば P I N を破棄することが出来る。

【0033】

図 7 は、本システムによりスマートカード 22 にアクセスを行うアプリケーション 21 の処理を示すフローチャートである。

尚これらの処理を行う機構をアプリケーション 21 に直接持たせる構成とすることも出来るが、これらの処理をライブラリとして実現し、このライブラリを各アプリケーション 21 に組込む形態を取るのが一般的な構成である。

【0034】

アプリケーション 21 は、スマートカード 22 にアクセスを行う際、まず排他制御機構 11 へ排他獲得の依頼を行い（ステップ S 1）、排他制御機構 11 からの応答を待つ。その結果、排他制御機構 11 から何等かの理由で、排他が獲得出来ない旨の通知が有れば（ステップ S 2、N O）、処理を終了する。

【0035】

排他獲得の依頼に対し、排他制御機構 11 から排他獲得成功の通知が有れば（ステップ S 2、Y E S）、次にステップ S 3 として、アクセス制御機構 12 にスマートカード 22 へのアクセスの開始宣言を行う。

【0036】

このスマートカード 22 へのアクセスが未認証のスマートカード 22 へのアクセスであり、スマートカード 22 への認証が必要なためアクセス制御機構 12 から P I N の入力を要求された時（ステップ S 4、Y E S）、ステップ S 8 としてアクセス制御機構 12 に P I N としてユーザが入力したパスワードをアクセス制御機構 12 に送って、認証処理を依頼し確認を行う。その結果認証されれば（ステップ S 9、Y E S）、処理をステップ S 5 に移してスマートカードへアクセスし、認証されなければ（ステップ S 9、N O）、処理を終了する。

【 0 0 3 7 】

ステップ S 4 において、このアクセスが既に認証を得ているスマートカード 2 2 へのアクセスである時（ステップ S 4、N O）、更なる認証処理は必要無いので、ステップ S 5 としてスマートカード 2 2 へのアクセスを許可してデータの読み出し／書込みを行う。

【 0 0 3 8 】

ステップ S 5 のアクセス処理が終了すると、ステップ S 6 として、アクセス制御機構 1 2 に対してスマートカード 2 2 へのアクセスの終了宣言を行う。そしてステップ S 7 として、そのスマートカード 2 2 への排他の解除を排他制御機構 1 1 に通知して処理をスマートカード 2 2 へのアクセス処理を終了する。

【 0 0 3 9 】

図 8 は、アプリケーション 2 1 からの排他獲得要求に対する排他制御機構 1 1 の処理を示すフローチャートである。

アプリケーション 2 1 から、スマートカード 2 2 への排他獲得要求があると、排他制御機構 1 1 は、ステップ S 1 1 として、排他獲得を要求されたスマートカード 2 2 が、既に他のアプリケーション 2 1 によって排他獲得済みであるかどうか判断される。その結果他のアプリケーション 2 1 による排他獲得が行われていなければ（ステップ S 1 1、N O）、そのスマートカード 2 2 を排他獲得済みとして登録し、要求を行ったアプリケーション 2 2 に排他獲得を通知して処理を終了する。

【 0 0 4 0 】

またステップ S 1 1 で他のアプリケーション 2 1 が排他獲得済みであるならば（ステップ S 1 1、Y E S）、ステップ S 1 2 としてこの排他獲得要求を排他待ちキューに追加して処理を終了する。

【 0 0 4 1 】

図 9 は、アプリケーション 2 1 からの排他の解除通知に対する排他制御機構 1 1 の処理を示すフローチャートである。

アプリケーション 2 1 からスマートカード 2 2 への排他の解除通知を受けると、排他制御機構 1 1 は、ステップ S 2 1 としてそのアプリケーション 2 2 の排他

獲得済みの登録を削除して排他を解除する。

【 0 0 4 2 】

そして排他待ちキューを調べ、排他が解除されたスマートカード 2 2 に対して排他待ちとなっているアプリケーション 2 1 が存在すれば（ステップ S 2 2、Y E S）、排他待ちキューの先頭に登録されているアプリケーション 2 1 のそのスマートカード 2 2 への排他獲得を登録してスマートカード 2 2 をディスパッチした後、また排他待ちキューに待ちが存在しなければ（ステップ S 2 2、N O）そのまま、処理を終了する。

【 0 0 4 3 】

図 1 0 は、アプリケーション 2 1 からのスマートカード 2 2 へのアクセス要求に対するアクセス制御機構 1 2 の処理を示すフローチャートである。

アプリケーション 2 1 からのアクセス開始宣言に対し、アクセス制御機構 1 2 は、ステップ S 3 1 として、認証状態管理テーブルにアプリ 1 を登録して、スマートカード 2 2 に対してアクセス要求プロセスを登録する。

【 0 0 4 4 】

図 1 1 は、アプリケーション 2 1 からのスマートカード 2 2 へのアクセス要求に対するアクセス制御機構 1 2 の処理を示すフローチャートである。

アプリケーション 2 1 からのアクセス要求に対し、アクセス制御機構 1 2 はステップ S 4 1 として認証状態管理テーブルを参照して、そのアプリケーション 2 1 がアクセス要求先のスマートカード 2 2 から既に認証済であるかどうか調べる。その結果、既に認証済みであれば（ステップ S 4 1、Y E S）、更なる認証は必要無いので、ステップ S 4 5 としてアプリケーション 2 1 に対してアクセス許可を通知する。

【 0 0 4 5 】

ステップ S 4 1 で、そのアプリケーション 2 1 がまだ認証を得ていないのならば（ステップ S 4 1、N O）、認証処理を行う必要があるので、ステップ S 4 2 としてアプリケーション 2 1 にパスワードの入力を要求し、スマートカード 2 2 に対して P I N による認証チェックを依頼する。その結果、スマートカード 2 2 から認証が得られれば、ステップ S 4 5 としてアプリケーション 2 1 に対してア

クセス許可を通知し、また認証が得られなければ（ステップ S 4 3、N O）、アクセス不許可をアプリケーション 2 1 に対して通知して処理を終了する。

【 0 0 4 6 】

図 1 2 は、本実施形態に於けるスマートカードを使用するシステムの構成を示す図である。

本実施形態でのアプリケーション 4 1 とスマートカード 4 2 との間を管理するアクセス管理システム 4 0 は、スマートカードリーダー 4 1 と各アプリケーション 4 1 のライブラリ 4 4 との間に構成され、O S の一機能として、あるいは O S に実装される形で実現される。

【 0 0 4 7 】

アプリケーション 4 1 は、スマートカード 4 2 に対する認証処理やアクセス処理を、全てこのアクセス制御システム 4 0 を介して行い、アクセス制御システム 4 0 は、各アプリケーション 4 1 とスマートカード 4 2 との間のやり取りを把握している。またアクセス制御システム 4 0 は、スマートカードリーダー 4 3 の状態も把握しており、例えばスマートカードリーダー 4 3 からスマートカード 4 2 が抜かれると、認証状態管理テーブルを調べ、そのカードが認証済みとしているアプリケーションがあれば未認証に変更する。

【 0 0 4 8 】

なお、アクセス管理システム 4 0 は、内部に排他制御機構 1 1 とアクセス制御機構 1 2 を別々に持つ構成となっているが、これらを 1 つの機能構成要素として実現することもできる。また、セキュリティ上、アクセス制御機構や排他制御機構は、複数のアプリケーションが共有できる必要があるので、O S のカーネル内に実現するとセキュリティをより向上することができる。

【 0 0 4 9 】

図 1 3 は、本実施形態における上記スマートカードのアクセス管理をコンピュータプログラムにより実現した場合の情報処理装置のシステム環境図である。

スマートカードを実装した情報処理装置は、図 1 3 の様に C P U 5 1、R O M、R A M による主記憶装置 5 2、補助記憶装置 5 3、ディスプレイ、キーボード等の入出力装置（I / O）5 4、L A N や W A N、一般回線等により他ノードと

ネットワーク接続を行うモデム等のネットワーク接続装置 5 5、ディスク、磁気テープなどの可搬記録媒体 5 7 から記憶内容を読み出す媒体読取り装置 5 6 及び 1 乃至複数のスマートカード 5 9 を実装しているスマートカードリーダー 5 8 を有し、これらが互いにバス 6 0 により接続される構成を備えている。

【 0 0 5 0 】

また図 1 3 の情報処理システムでは、媒体読取り装置 5 6 により磁気テープ、フロッピーディスク、CD-ROM、MO 等の記録媒体 5 7 に記憶されているプログラム、データを読み出し、これを主記憶装置 5 2 またはハードディスク 5 5 にダウンロードする。そして本実施形態による各処理は、CPU 5 1 がこのプログラムやデータを実行することにより、ソフトウェア的に実現することが可能である。

【 0 0 5 1 】

また、この情報処理装置では、フロッピーディスク等の記録媒体 5 7 を用いてアプリケーションソフトの交換が行われる場合がある。よって、本発明は、計測制御用監視端末やその画面の操作方法に限らず、コンピュータにより使用されたときに、上述の本発明の実施の形態の機能をコンピュータに行わせるためのコンピュータ読み出し可能な記録媒体 5 7 として構成することもできる。

【 0 0 5 2 】

この場合、「記録媒体」には、例えば図 1 4 に示されるように、CD-ROM、フロッピーディスク（あるいは MO、DVD、リムーバブルハードディスク等であってもよい）等の媒体駆動装置 7 7 に脱着可能な可搬記録媒体 7 6 や、ネットワーク回線 7 3 経由で送信される外部の装置（サーバ等）内の記憶手段（データベース等）7 2、あるいは情報処理装置 7 1 の本体 7 4 内のメモリ（RAM 又はハードディスク等）7 5 等が含まれる。可搬記録媒体 7 6 や記憶手段（データベース等）7 2 に記憶されているプログラムは、本体 7 4 内のメモリ（RAM 又はハードディスク等）7 5 にロードされて、実行される。

【 0 0 5 3 】

（付記 1） 複数のアプリケーションによるスマートカードへのアクセスを管理するスマートカードのアクセス管理システムであって、

アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャンネルが存在すれば、該アプリケーションを排他獲得済みとする排他制御手段と

排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可するアクセス制御手段と

を備えることを特徴とするアクセス管理システム。

【 0 0 5 4 】

(付記 2) 前記排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャンネルが存在しなければ、該排他獲得要求を行ったアプリケーションをキューに登録することを特徴とする付記 1 に記載のアクセス管理システム。

【 0 0 5 5 】

(付記 3) 前記アクセス制御手段は、前記アクセス要求に対し、前記排他を獲得したアプリケーションが前記スマートカードから未認証である時、該アプリケーションの要求を拒絶することを特徴とする付記 1 又は 2 に記載のアクセス管理システム。

【 0 0 5 6 】

(付記 4) 前記アクセス制御手段は、アプリケーションとスマートカードとの認証関係を該アプリケーションのプロセス ID を用いて管理することを特徴とする付記 1 乃至 3 のいずれか 1 に記載のアクセス管理システム。

【 0 0 5 7 】

(付記 5) 前記アクセス制御手段は、前記スマートカードがスマートカードリーダーより抜かれた時、該抜かれたスマートカードにより認証済みとなっているアプリケーションを未認証に変更することを特徴とする付記 1 乃至 4 のいずれか 1 に記載のアクセス管理システム。

【 0 0 5 8 】

(付記 6) 前記アプリケーションは、前記スマートカードに複数回アクセスする時、各アクセスの開始時に前記排他制御手段に前記排他獲得要求を行い、該各アクセスの終了時に前記排他制御手段に排他の解除通知を行うことを特徴とする付記 1 乃至 5 のいずれか 1 に記載のアクセス管理システム。

【 0 0 5 9 】

(付記 7) 前記排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードが他のアプリケーションによって既に排他獲得済みであれば、該排他獲得要求を行ったアプリケーションをキューに登録し、前記アプリケーションからの排他の解除通知に対し、前記キューに登録されているアプリケーションを排他獲得済みとすることを特徴とする付記 6 に記載のアクセス管理システム。

【 0 0 6 0 】

(付記 8) 前記アクセス制御手段は、アプリケーションからスマートカードの認証解除の通知に対し、該認証解除が該スマートカードにより認証済みとなっている最後のアプリケーションからの時、該スマートカードに認証解除を要求することを特徴とする付記 1 乃至 7 のいずれか 1 に記載のアクセス管理システム。

【 0 0 6 1 】

(付記 9) 複数のアプリケーションによるスマートカードへのアクセスを管理するスマートカードの共有方法であって、

アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとし、

排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可することを特徴とする共有方法。

【 0 0 6 2 】

(付記 1 0) 1 つのスマートカードへの複数のアクセス処理を含むアプリケ

ーション又はそのライブラリであって、

前記各アクセス処理に対し、該アクセス処理の開始時にそれぞれ前記排他獲得要求を行い、各アクセス処理の終了時にそれぞれ排他の解除通知し、

前記複数のアクセス処理のうちの最初の処理時のみに該アクセス処理を行うスマートカードに対して認証要求を行うことを特徴とするアプリケーション又はそのライブラリ。

【 0 0 6 3 】

(付記 1 1) 1 つスマートカードへの複数のアクセス処理を含むアプリケーションのライブラリであって、

前記各アクセス処理に対し、該アクセス処理の開始時にそれぞれ前記排他獲得要求を行い、各アクセス処理の終了時にそれぞれ排他の解除通知し、

前記複数のアクセス処理のうちの最初の処理時のみに該アクセス処理を行うスマートカードに対して認証要求を行うことを特徴とするアプリケーションのライブラリ。

【 0 0 6 4 】

(付記 1 2) 複数のアプリケーションが並列動作する情報処理装置によって使用された時、

アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャンネルが存在すれば、該アプリケーションを排他獲得済みとし、

排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可することを前記情報処理装置に行わせるプログラムを記憶した前記情報処理装置が読み出し可能な記録媒体。

【 0 0 6 5 】

【発明の効果】

本発明によれば、排他制御によりスマートカードに対する排他制御が行われるので、複数のアプリケーションによってスマートカードを共用しても各アプリケ

ーション単位の認証を可能とする。

【 0 0 6 6 】

また、各アプリケーションとスマートカードとの間の認証関係が一元管理されているので、アプリケーションがスマートカードにアクセス要求を行うとそのスマートカードはそのアプリケーションを認証済みかどうか判断され、未認証の場合のみ認証処理が行われるので、認証処理回数を削減することが出来、認証処理によるオーバーヘッドを小さくすることが出来る。また P I N による認証処理は、最初に一度だけ行われるのでアプリケーションは、P I N を保持し続ける必要がなく、セキュリティレベルの向上が図れる。

【 0 0 6 7 】

更にスマートカードは、認証状態を保持したまま複数の認証済みアプリケーションとの間でアクセスが可能となる。

またアプリケーションは、排他獲得の為の待ち状態期間を短く出来る。よって処理の並列性を向上出来また各アプリケーションの処理時間の短縮を図れる。

【図面の簡単な説明】

【図 1】

排他制御機構を設け、スマートカードへのアクセスの排他処理を行った場合の構成を示す図である。

【図 2】

排他制御機構を備えた構成時の各アプリケーションへのスマートカードへのアクセス処理を示す図である。

【図 3】

排他制御機構及びアクセス制御機構を設けた場合の構成図である。

【図 4】

認証状態管理テーブルの構成例を示す図である。

【図 5】

アプリケーションがスマートカードへのアクセスを行う際の、アプリケーション、排他制御機構及びアクセス制御機構の処理の流れを示した図である。

【図 6】

排他制御機構及びアクセス制御機構を備えた構成時の各アプリケーションへのスマートカードへのアクセス処理を示す図である。

【図 7】

スマートカードにアクセスを行うアプリケーションの処理を示すフローチャートである。

【図 8】

アプリケーションからの排他獲得要求に対する排他制御機構の処理を示すフローチャートである。

【図 9】

アプリケーションからの排他の解除通知に対する排他制御機構の処理を示すフローチャートである。

【図 1 0】

アプリケーションからのスマートカードへのアクセス開始宣言に対するアクセス制御機構の処理を示すフローチャートである。

【図 1 1】

アプリケーションからのスマートカードへのアクセス要求に対するアクセス制御機構の処理を示すフローチャートである。

【図 1 2】

本実施形態に於けるスマートカードを使用するシステムの構成を示す図である。

【図 1 3】

情報処理装置のシステム環境図である。

【図 1 4】

記憶媒体の例を示す図である。

【図 1 5】

スマートカード内部の論理的構成を示す図である。

【符号の説明】

- 1 1 排他制御機構
- 1 2 アクセス制御機構

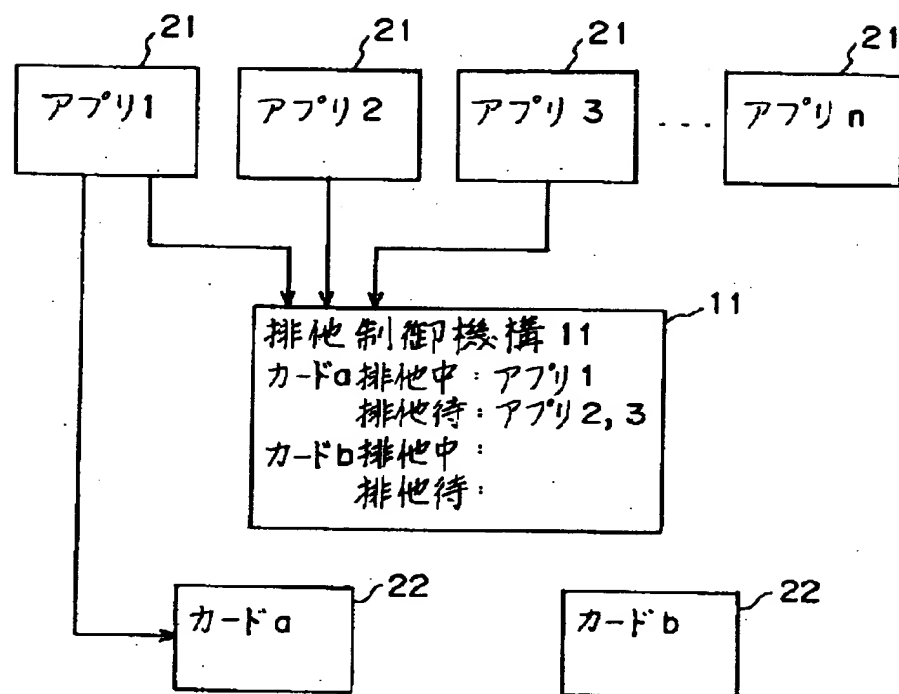
- 2 1、4 1 アプリケーション
- 2 2、4 2、5 9 スマートカード
- 4 0 アクセス制御システム
- 4 3、5 8 スマートカードリーダー
- 5 1 CPU
- 5 2 主記憶装置
- 5 5 補助記憶装置
- 5 4 入出力装置
- 5 5 ネットワーク接続装置
- 5 6 媒体読取り装置
- 5 7 可搬記憶媒体
- 6 0 バス
- 7 1 情報処理装置
- 7 2 記憶手段
- 7 3 ネットワーク回線
- 7 4 情報処理装置本体（コンピュータ）
- 7 5 メモリ
- 7 6 可搬記録媒体

【書類名】

図面

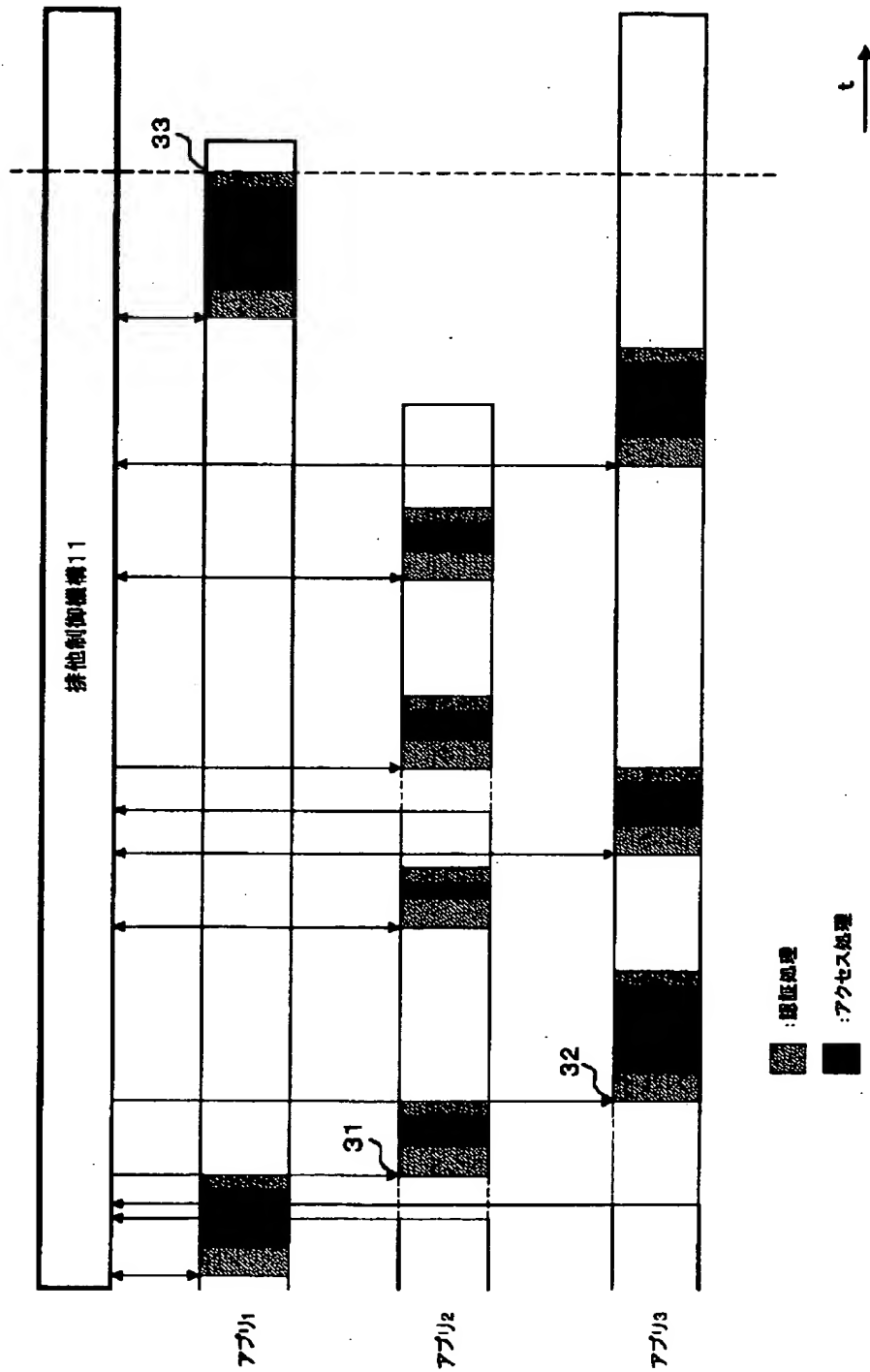
【図 1】

排他制御機構を設け、スマートカードへのアクセスの排他処理を行った場合の構成を示す図



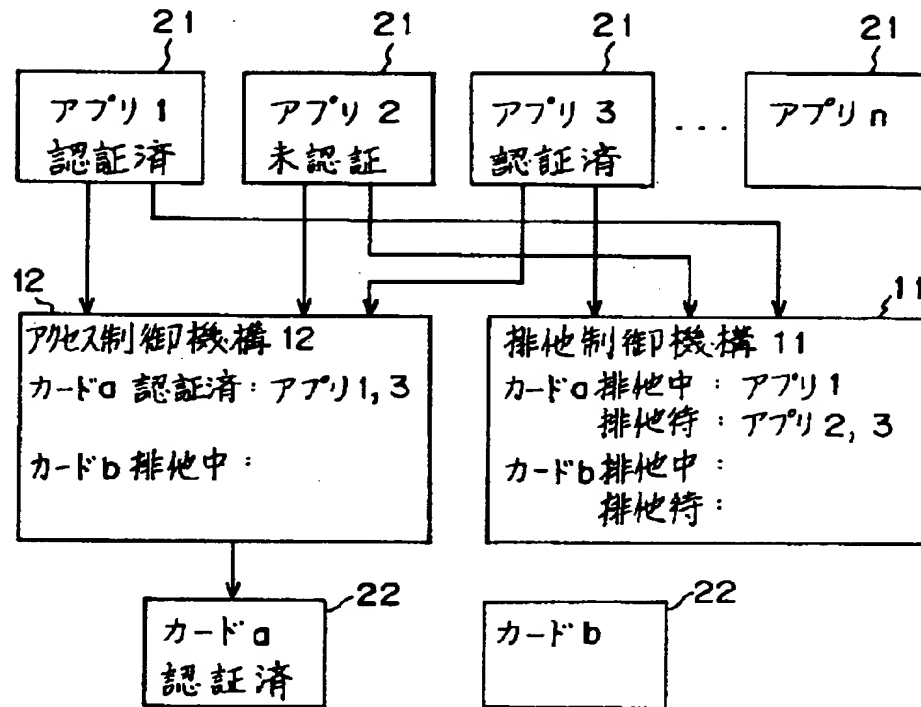
【図2】

排他制御機構を備えた構成時の各アプリケーション
へのスマートカードへのアクセス処理を示す図



【図 3】

排他制御機構及びアクセス制御機構を
設けた場合の構成図



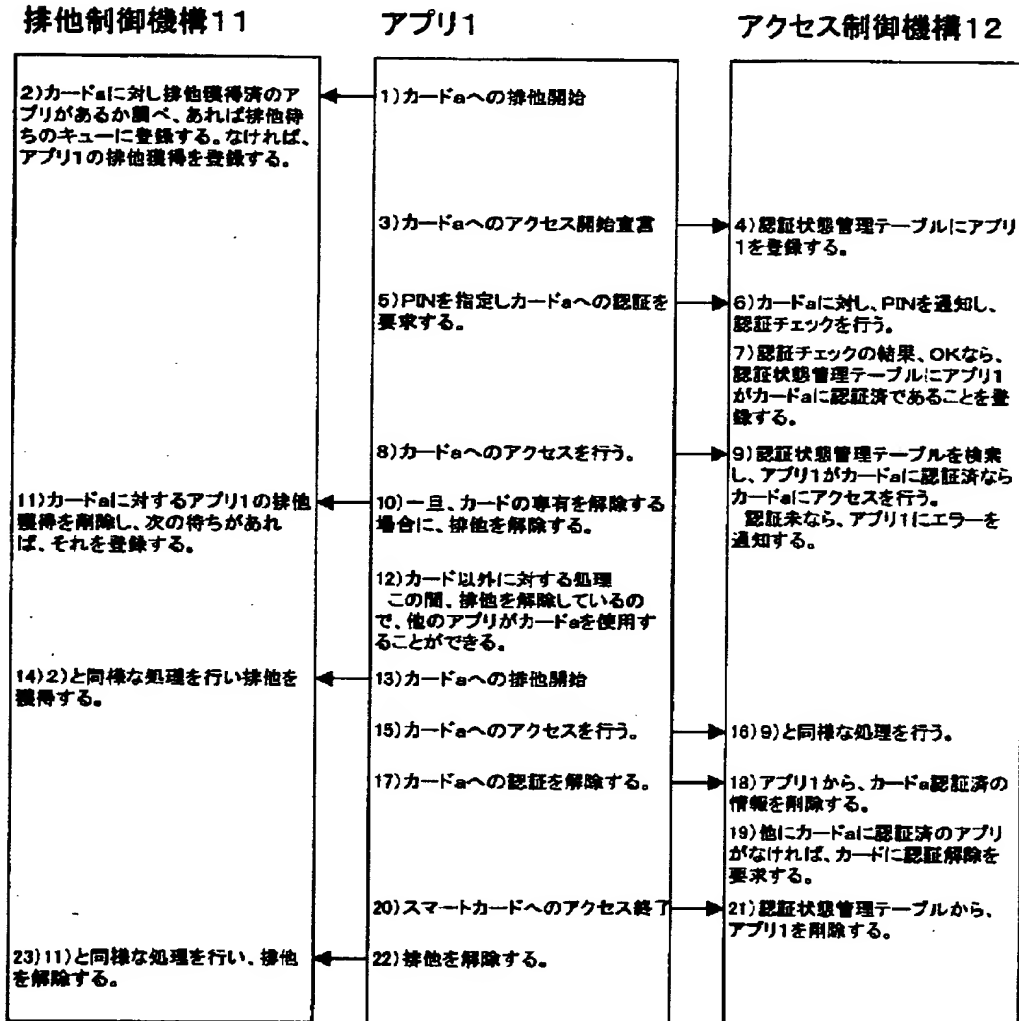
【図 4】

認証状態管理テーブルの
構成例を示す図

アプリ識別情報	認証済みカード情報	
アプリ1	カードa	カードb
アプリ2		
アプリ3	カードa	
.....
アプリn		

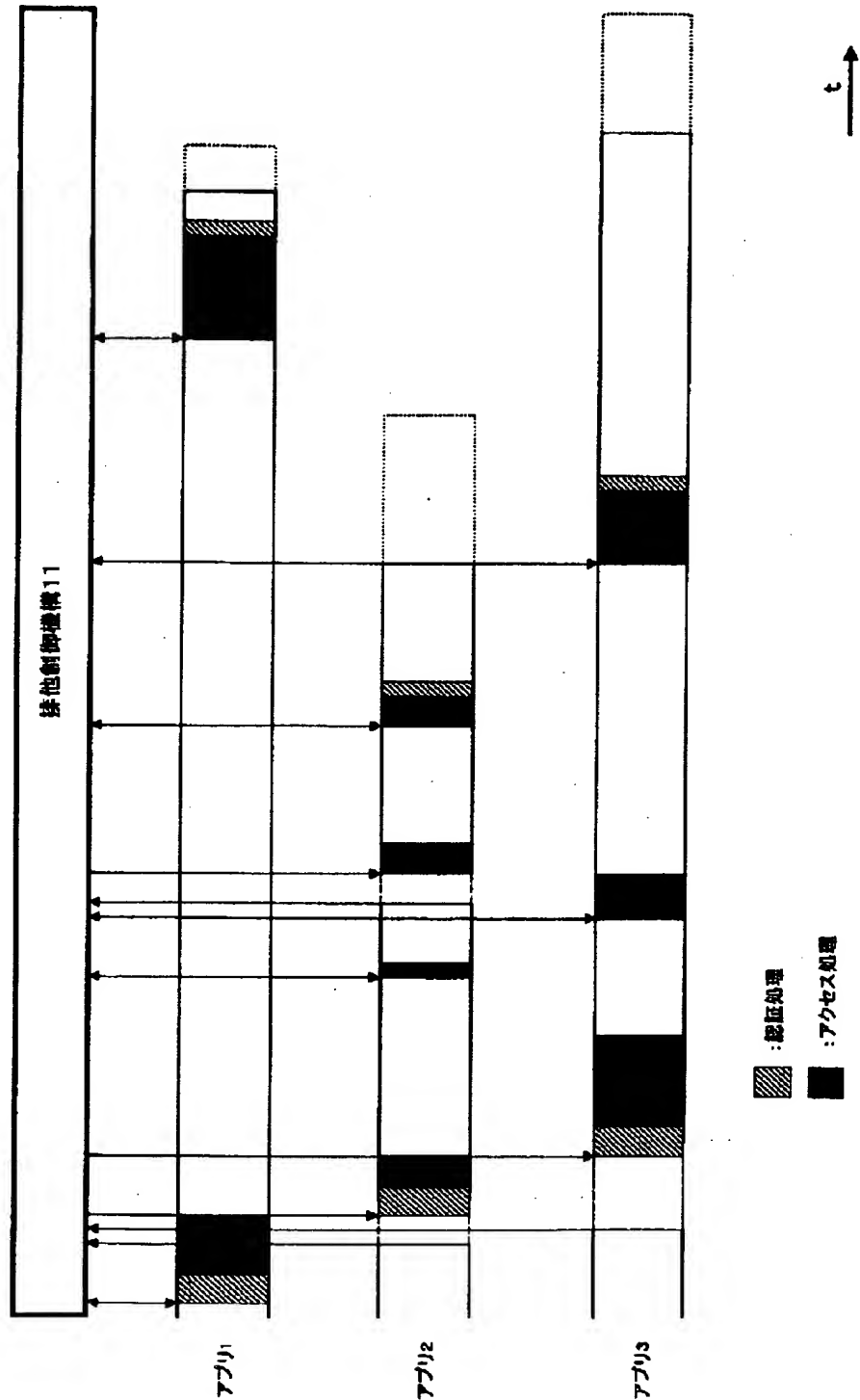
【図 5】

アプリケーションがスマートカードへのアクセスを行う際の、アプリケーション、
排他制御機構及びアクセス制御機構の処理の流れを示した図



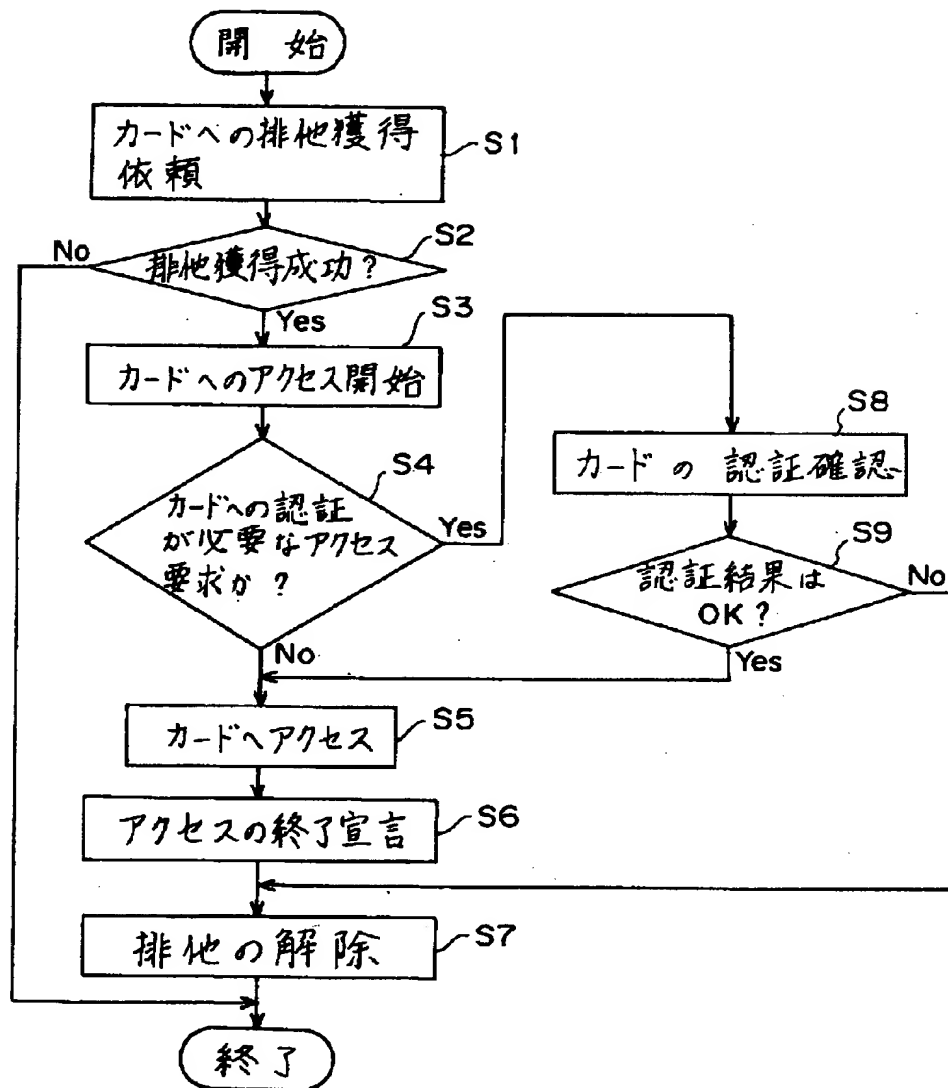
【図6】

排他制御機構及びアクセス制御機構を備えた構成時の
各アプリケーションへのスマートカードへのアクセス処理を示す図



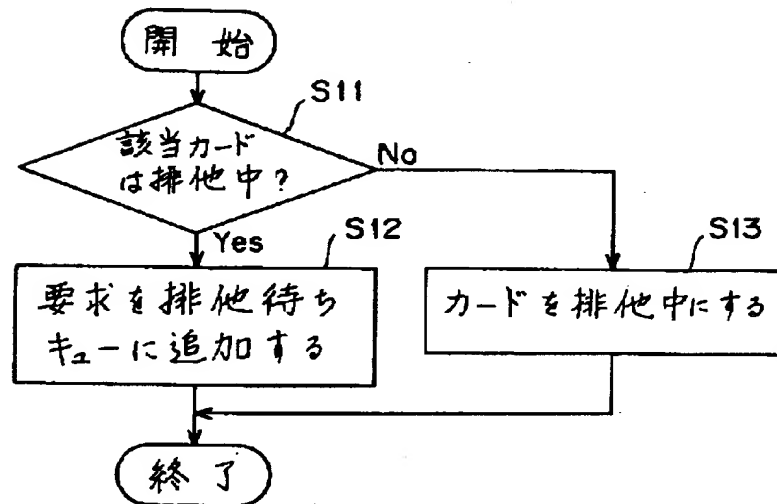
【図 7】

スマートカードにアクセスを行うアプリケーションの
処理を示すフローチャート



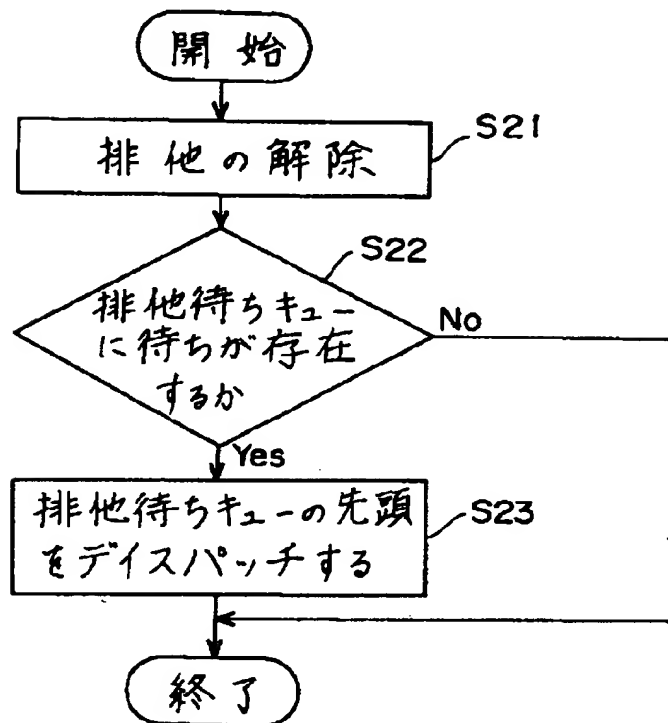
【図 8】

アプリケーションからの排他獲得要求に対する
排他制御機構の処理を示すフローチャート



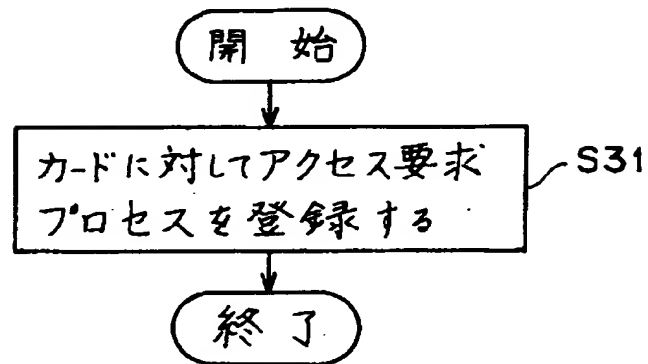
【図 9】

アプリケーションからの排他の解除通知に
対する排他制御機構の処理を示す
フローチャート



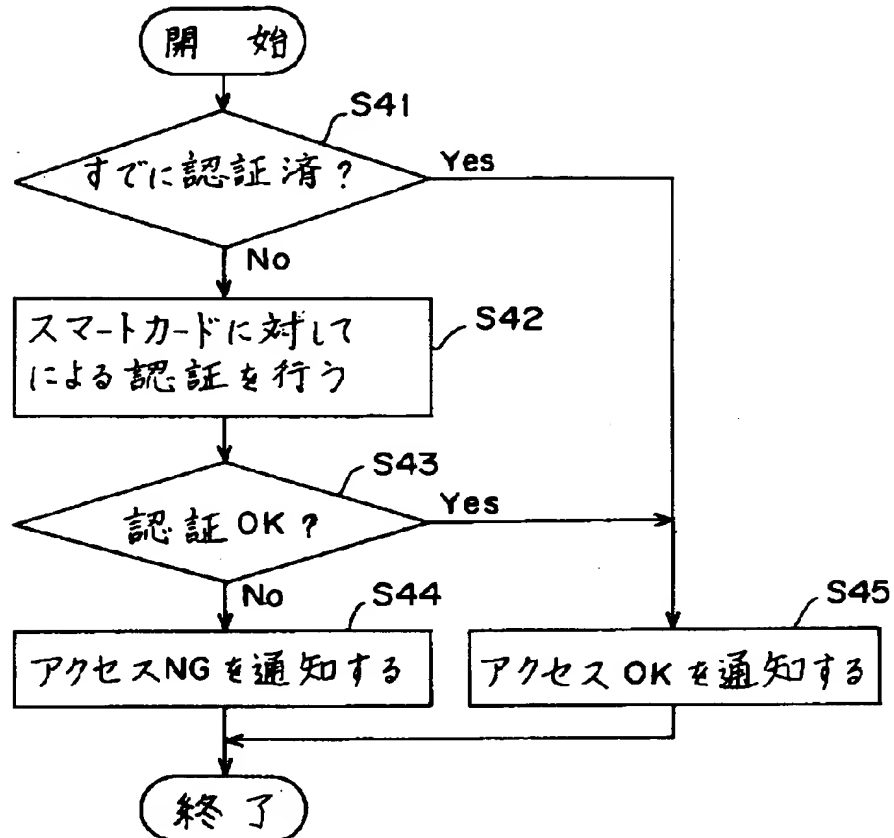
【図10】

アプリケーションからのスマートカードへの
アクセス開始宣言に対するアクセス
制御機構の処理を示すフローチャート



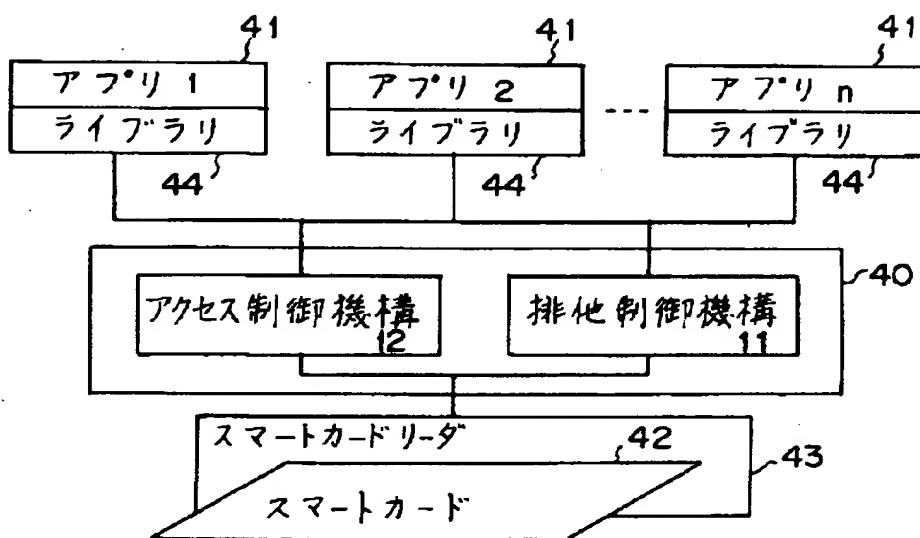
【図 11】

アプリケーションからのスマートカードへのアクセス要求に
対するアクセス制御機構の処理を示すフローチャート



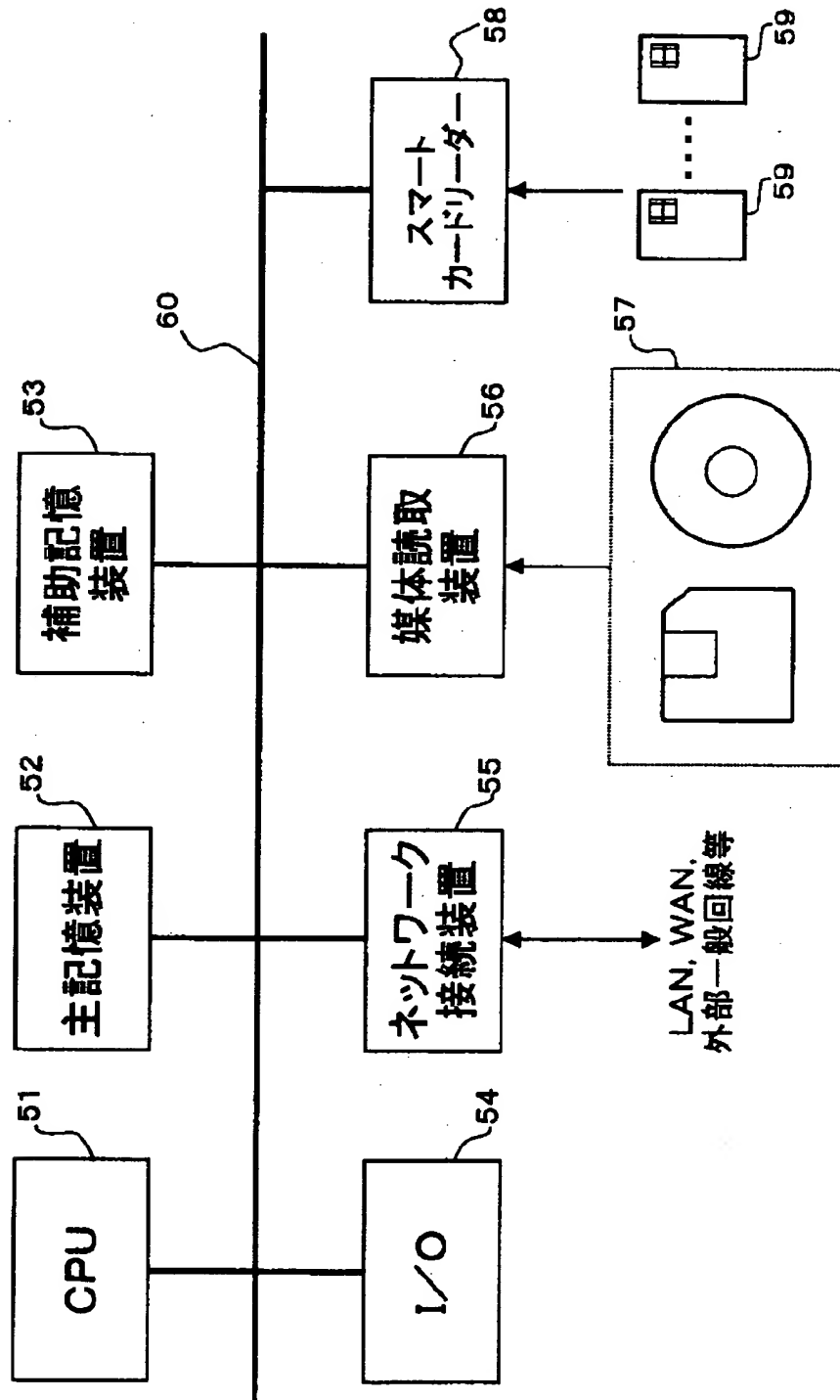
【図12】

本実施形態に於けるスマートカードを使用する
システムの構成を示す図



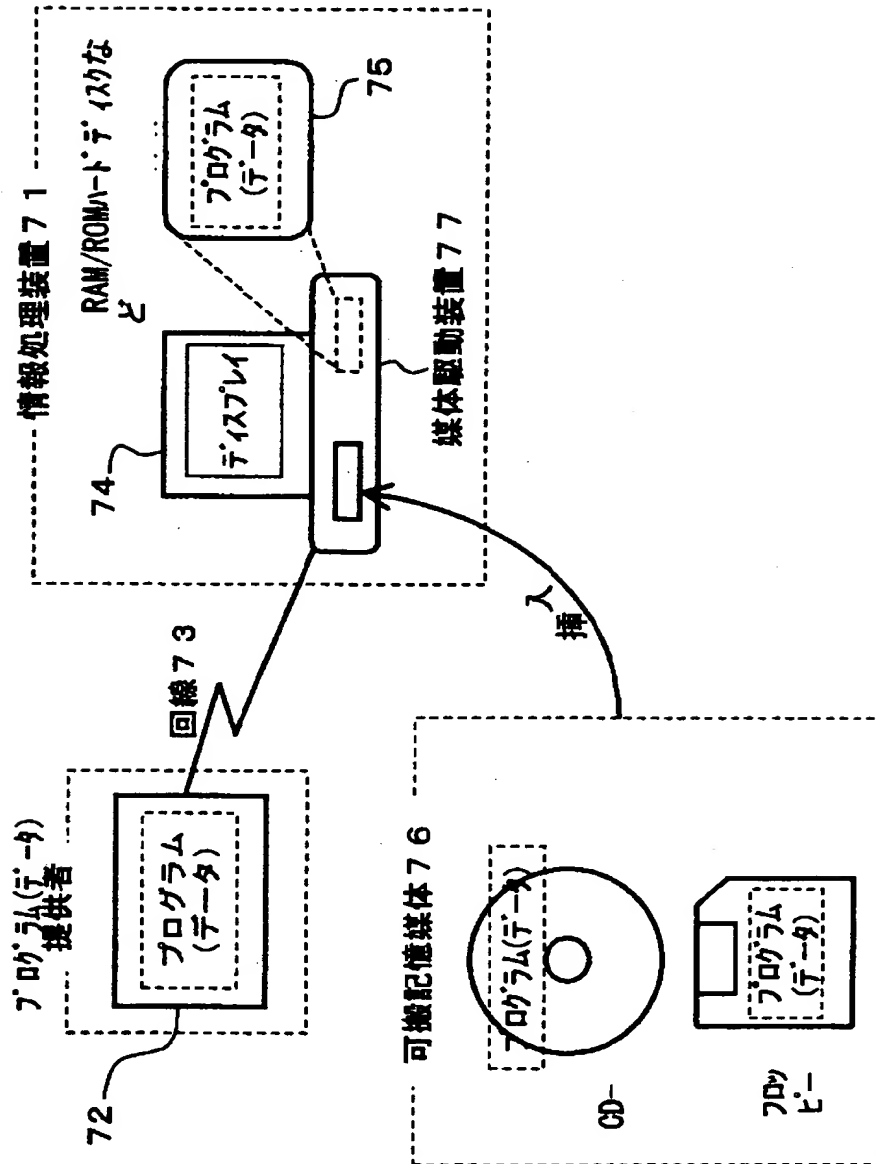
【図 13】

情報処理のシステム環境図



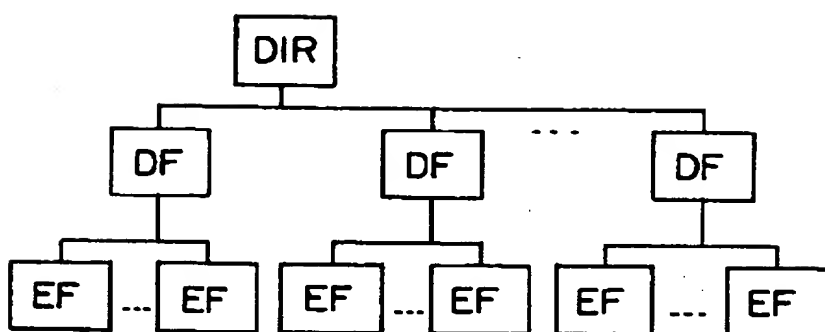
【図 14】

記憶媒体の例を示す図



【図 1 5】

スマートカード内部の論理的構成を
示す図



【書類名】 要約書

【要約】

【課題】 複数のアプリケーションによるアクセスに対し、各アプリケーション（プロセス）毎に認証許可を与えるスマートカードのアクセス管理システム及び管理方法を提供することを課題とする。

【解決手段】 スマートカードへの複数のアクセス処理を含むアプリケーション 2 1 は、各アクセス処理毎にスマートカード 2 2 に対してアクセス要求を行う際、排他制御機構 1 1 に対して排他獲得要求を行い、排他が得られるとアクセス制御機構 1 2 に対してアクセスを要求する。アクセス制御機構 1 2 はアプリケーション 2 1 が未認証ならば P I N の入力进行要求し、既に認証を得られていればスマートカード 2 2 へのアクセスを許可する。アプリケーション 2 1 はアクセス処理単位で排他獲得要求／解除を行う。

【選択図】 図 3

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日	1996年 3月26日
[変更理由]	住所変更
住 所	神奈川県川崎市中原区上小田中4丁目1番1号
氏 名	富士通株式会社